



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,793	04/13/2001	Jung-Wan Ko	1293.1191	1932

49455 7590 02/24/2006

STEIN, MCEWEN & BUI, LLP  
1400 EYE STREET, NW  
SUITE 300  
WASHINGTON, DC 20005

EXAMINER

PICH, PONNOREAY

ART UNIT

PAPER NUMBER

2135

DATE MAILED: 02/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/833,793	KO ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 09 December 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1,3-11,13-18,20-30,32-35 and 41-45 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,3-11,13-18,20-30,32-35 and 41-45 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |                                                                                                    |                                                                             |
|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                                   | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____                                                |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>12/2005</u> .                                                             | 6) <input type="checkbox"/> Other: _____                                    |

### **DETAILED ACTION**

Claims 1, 3-11, 13-18, 20-30, 32-35, and 41-45 are pending. Any objections or rejections not repeated below for record are withdrawn due to applicant's amendments and/or arguments.

#### ***Information Disclosure Statement***

Applicant's IDS submitted on 12/9/2005 has been considered.

#### ***Response to Arguments***

Applicant's arguments have been considered. Not all of applicant's arguments were persuasive. As per the rejections or objections in which applicant's arguments were persuasive, the rejections or objections have been withdrawn. As per the arguments which were not persuasive, the examiner respectfully traverses applicant's arguments. The examiner notes that many of applicant's art arguments are substantially similar. As such, the examiner will only address the unique art arguments.

As per claim 41, applicant argues that claim 41 is statutory because it is drawn to a receiver for receiving encrypted text and therefore is a device claim and not software alone as alleged by the examiner. Applicant argues claim 41 is considered functional descriptive material.

The examiner respectfully disagrees. Devices can be hardware, software, or a combination of hardware and software. Absent any recitation of hardware in the claim, the receiver device of claim 42 reads on software per se, which is not statutory. Further, it makes no sense for applicant to argue that claim 41 is considered functional descriptive material and say that the claim 41 is device claim, which the examiner

Art Unit: 2135

assumes applicant is trying to argue that the receiver of claim 41 is a hardware device. Whether going by the old 101 guidelines or the new guidelines recently issued by the Office, if one of ordinary skill in the art at the time applicant's invention could have reasonably interpreted claim 41 as being directed to software per se, claim 41 is not statutory. Applicant must explicitly recite hardware in the receiver of claim 41 or define the receiver of claim 41 as hardware, i.e. see claims 43-44, for claim 41 to be statutory since from page 9, paragraph 29 of the specification, it would appear that the receiver of claim 41 reads on software per se, i.e. a server comprising a software-implemented authenticator and a software-implemented decryptor.

Applicant argues that instead of teaching encrypting a first region of a text containing a second encryption key using a first encryption key and encrypting a second region of the text using the second encryption key, Orrin instead teaches encrypting a first region of text containing a second encryption key using a first encryption key and encrypting a second region of the text using the second encryption key. The examiner respectfully submits that the labels of what is the first encryption key and what is the second encryption key is arbitrary and does not matter. What applicant calls the first encryption key disclosed by Orrin reads on the second encryption key recited in applicant's claimed invention and what applicant calls the second encryption key disclosed by Orrin reads on the first encryption key recited in applicant's claimed invention. Applicant appears to be arbitrarily labeling the public key and user local key of Orrin as the second and third key. They could have just as easily been labeled as the first key. Likewise, the session key could have just as easily been labeled as the

Art Unit: 2135

second key rather than the first key. As such, the examiner respectfully submits that Orrin teaches the limitations in contention since the session key, i.e. the second encryption key, is used to encrypt the second region of the text and the public key or the user local key, i.e. the first encryption key, is used to encrypt the first region of the text containing the second encryption key, i.e. the header of the text.

Applicant argues Orrin does not teach decrypting the first region of the cipher text using the transmitted first encryption key and the transmitted region segmentation information; extracting the second encryption key from the decrypted first region using the transmitted second encryption key information; and decrypting the second region of the text using the extracted second encryption key. Applicant noted that the examiner relied upon Orrin's teachings that a decryption method is generally the equivalent of an encryption operation in reverse to reject these limitations. Applicant argues that because Orrin instead teaches encryption by which data is encrypted using a first key, encrypting the first key using a second key, and adding a header to the encrypted data, Orrin's decryption method would instead consist of decrypting the first key using the second key and decrypting the data with the first key. The examiner has addressed how the labeling of what is the "first encryption key" and "the second encryption key" as applied to Orrin's teachings is an arbitrary matter, therefore the traversal of applicant's arguments that Orrin's decryption method is not what is recited in the claims flows from the traversal of applicant's arguments that Orrin's encryption method is not what is recited in the claims.

Art Unit: 2135

The rest of applicant's arguments with regards to art rejections are directed towards dependency and that the secondary art used in the rejections do not overcome the deficiency of Orrin with regards to the limitations in the independent claim that applicant had argued Orrin does not teach. As the examiner has traversed the arguments in the independent claims, applicant's arguments for the dependent claims are moot.

### ***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 41 and 45 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

#### **Claim 41:**

Claim 41 recites a receiver for receiving encrypted text comprising an authenticator and a decryptor. The examiner notes that on page 9, paragraph 29 of the specification, a receiver is defined such that it may consist of a computer, a server, or an information appliance. A server refers to just software. Hence, claim 41 reads on a software receiver. Software by itself is non-statutory.

#### **Claim 45:**

Claim 45 defines the receiver of claim 42 as a server. As mentioned, a server reads on software alone. Nothing statutory is recited.

The examiner notes that claims 43 and 44 define the receiver as an information appliance and a computer respectively, which defines the receiver as a specific type of hardware. Hence, claims 43 and 44 are statutory.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 3-4, 7, 8, 10-11, 16, 13, 18, 21, 24-25, 27, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orrin (US 6,011,849).

#### **Claim 1:**

As per claim 1, Orrin discloses the limitations of:

1. Encrypting a first region of a text containing a second encryption key using a first encryption key (col 7, line 62-col 8, line 8).
2. Encrypting a second region of the text using the second encryption key (col 4, lines 10-15 and col 7, lines 59-62).
3. Transmitting a cipher text comprising the encrypted first and second regions (col 3, lines 18-21).
4. Transmitting the first encryption key (col 8, lines 9-12).

Orrin does not explicitly recite the limitations of:

1. Transmitting region segmentation information for segmenting the text into the first region and the second region and information related to the second encryption key.
2. Decrypting the first region of the transmitted cipher text using the transmitted first encryption key and the transmitted region segmentation information.
3. Extracting the second encryption key from the decrypted first region using the transmitted information related to the second encryption key.
4. Decrypting the second region of the transmitted cipher text using the extracted second encryption key.

However, Orrin discloses that among the information sent in the header are the minimum information needed to decrypt the header and message cipher text (col 8, lines 3-8). Orrin further discloses that every encryption method also includes a decryption capability; the decryption is generally the equivalent of the encryption operation in reverse (col 9, lines 34-36). The examiner submits that these teachings by Orrin read on the above limitations which Orrin does not explicitly recite. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Orrin's invention according to the limitations recited in claim 1 because decryption is generally the reverse of the encryption operation and to decrypt the cipher text which were encrypted using the encryption steps as recited in claim 1,



Art Unit: 2135

the receiver would need information relating to the region segmentation information and the second encryption key.

**Claim 3:**

Orrin further discloses wherein the first encryption key comprises an encryption key for use with a common key encryption method (col 7, lines 59-67).

**Claim 4:**

Orrin further discloses wherein the first encryption key comprises a public key for use with a public key encryption method (col 7, lines 59-67).

**Claim 7:**

Orrin does not explicitly recite wherein the information related to the second encryption key includes size and position information of the second encryption key. However, this limitation must exist in Orrin's invention as he discloses that the header contains information needed to decrypt the message (col 8, lines 3-8). Without information related to the size and position of the second encryption key, decryption would be impossible.

**Claim 8:**

Orrin does not explicitly disclose wherein the position and size information of the second encryption key are fixed. However, this limitation is obvious to Orrin's invention. Orrin discloses that the header contains the minimum information needed to decrypt the cipher text and that this information is located in the clear text area of the header (col 8, lines 3-8). Being located in the clear text area always reads on the position and size information of the second encryption key being fixed.

**Claim 10:**

Orrin further discloses the first region of the text is smaller than the second region of the text (col 7, line 62-col 8, line 8). Note that the first region is the header and the second region is the rest of the text. File headers are typically smaller than the rest of the file.

**Claim 11:**

Orrin does not explicitly disclose wherein the region segmentation information comprises information on a starting address of the second region of the text. However, as mentioned, Orrin teaches the header containing the minimum information needed to decrypt the cipher text (col 8, lines 3-8). This minimum information must comprise region segmentation information which comprises information on a starting address of the second region of the text or decryption would not be possible if the decryptor does not know where the second region starts.

**Claim 16:**

Orrin does not explicitly disclose wherein the region segmentation information comprises information on a size of the first region of the text. However, Orrin teaching the header information containing the minimum information needed to decrypt the header and the rest of the cipher text reads on this limitation as this information is needed to decrypt the header (col 8, lines 3-8).

**Claim 13:**

Orrin discloses a sender who encrypts a first region of a text containing a second encryption key information using a first encryption key (col 7, line 62-col 8, line 12),

Art Unit: 2135

encrypts a second region of the text using a second encryption key based upon the second encryption key information (col 4, lines 10-15 and col 7, lines 59-62), and transmits the cipher text, first encryption key, region segmentation information, and the second encryption key information to a receiver (col 7, line 62-col 8, line 12 and col 9, lines 34-36). Note that for decryption to be successful, the sender of Orrin's invention must send to the receiver region segmentation information and the second encryption key information.

Orrin does not explicitly disclose the limitations of:

1. Decrypting the first region of the cipher text using the transmitted first encryption key and the transmitted region segmentation information.
2. Extracting the second encryption key from the decrypted first region using the transmitted second encryption key information.
3. Decrypting the second region of the text using the extracted second encryption key.

However, these limitation are substantially similar to the ones discussed in claim 1 as being obvious to Orrin's invention and are rejected for the same reasons.

**Claim 18:**

Orrin discloses the limitations of:

1. Encrypting a second region of the text using a first encryption key, where the first region contains a second encryption key (col 7, line 62-col 8, line 8).

Art Unit: 2135

2. Encrypting a second region of the text using the second encryption key (col 4, lines 10-15 and col 7, lines 59-62).
3. Transmitting the first encryption key (col 8, lines 9-12).

Orrin does not explicitly recite the limitations of:

1. Transmitting regions segmentation information for segmenting the text into the first region and the second region.
2. Decrypting the first region of the text using the first encryption key and the transmitted region segmentation information.
3. Extracting the second encryption key from the decrypted first region.
4. Decrypting the second region of text using the extracted second encryption key.

However, Orrin discloses that among the information sent in the header are the minimum information needed to decrypt the header and message ciphertext (col 8, lines 3-8). Orrin further discloses that every encryption method also includes a decryption capability; the decryption is generally the equivalent of the encryption operation in reverse (col 9, lines 34-36). The examiner submits that these teachings by Orrin read on the above limitations which Orrin does not explicitly recite. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Orrin's invention according to the limitations recited in claim 13 because decryption is generally the reverse of the encryption operation and to decrypt the cipher text which were encrypted using the encryption steps as recited in claim 13,

the receiver would need information relating to the region segmentation information and the second encryption key.

**Claim 21:**

Orrin further discloses wherein the first encryption key comprises an asymmetric key for use with an asymmetric key encryption method (col 7, line 62-col 8, line 8).

**Claim 24:**

Claim 24 recites a limitation substantially similar to what is recited in claim 7 and is rejected for the same reasons.

**Claim 25:**

Claim 25 recites a limitation substantially similar to what is recited in claim 8 and is rejected for the same reasons.

**Claim 27:**

Claim 27 recites a limitation substantially similar to what is recited in claim 10 and is rejected for the same reasons.

**Claim 30:**

As per claim 30, Orrin does not explicitly disclose the limitations of:

1. Decrypting a first region of the encrypted text using a first encrypted encryption key, where the region contains a second encryption key.
2. Decrypting a second region of the encrypted text using the second encryption key.
3. Decryption the first region using region segmentation information.

4. Extracting the second encryption key from the decrypted first region using information related to the second encryption key.

However, Orrin discloses that decryption is generally the reverse of the encryption operation (col 9, lines 34-36). The examiner submits that the above limitations are obvious to Orrin's invention in light of the encryption method discussed in claim 1. One of ordinary skill would have been motivated to use the above recited decryption method in Orrin's invention as they are the steps necessary to decrypt the encrypted cipher text encrypted using Orrin's invention and are essentially the reverse steps of the encryption operation.

Claims 5, 17, 15, 20, 22, 28-29, 32-33, 35, and 41-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orrin (US 6,011,849) in view of applicant's admittance of prior art.

**Claim 5:**

Orrin does not explicitly disclose wherein the second encryption key is smaller than the first encryption key where a common key encryption method is used. However, note that in Orrin's invention, both a common and public encryption key is used (col 7, lines 59-67). The public key, i.e. the first key, is used to encrypt the common key, i.e. the session key or second key. Further, the examiner asserts it was

Art Unit: 2135

well known in the art for common keys to be smaller in comparison to public keys. This allows common key encryptions to generally be faster than public key encryptions.

Applicant also admits that it was known in the prior art at the time the applicant's invention was made that common keys are typically smaller in comparison with a public key (see applicant's specification, p4-5, paragraph 13). Therefore, the limitation recited in claim 5 is obvious to Orrin's invention. One of ordinary skill would have been motivated to have the second encryption key be smaller than the first encryption key where a common key encryption method is used as this allows for faster encryption processing with the second key.

**Claim 17:**

Orrin does not explicitly disclose wherein the first encryption key comprises an encryption key that is 56 bits or more. However, Orrin discloses the first encryption key is a public encryption key (col 7, line 62-col 8, line 8). Applicant discloses that it was well known in the art that public encryption key methods that the keys are at least 512 bits (see specification, page 1, paragraph 3). It would have been obvious to one of ordinary skill in the art to have made the first encryption key of Orrin's invention at 56 bits or more. One of ordinary skill would have been motivated to do so as public keys are typically longer than 56 bits to offer greater security.

**Claim 15:**

Claim 15 recites limitations that are a combination of what are recited in claims 5 and 10 and are rejected for the same reasons. Note that there is a slight difference in the wording of the limitation of claim 5 and a limitation recited in claim 15. Claim 5

Art Unit: 2135

recites that the second encryption key is smaller than the first encryption key while claim 15 recites that the size of the first encryption key is larger than the size of the second encryption key. The meaning is essentially the same, however.

**Claim 20:**

Orrin does not explicitly disclose wherein the first encryption key comprises a symmetric key having 56 bits or more. However, applicant discloses it was well known in the art that symmetric keys typically are 40 or 56 bits. It would have been obvious to one of ordinary skill in the art to have modified Orrin's invention according to the limitations recited in claim 20 because it would allow for a faster encryption method than with public key cryptography.

**Claim 22:**

Claim 22 recites a limitation substantially similar to what is recited in claim 5 and is rejected for the same reasons.

**Claim 28:**

Orrin does not explicitly disclose sending information on a starting address of the second region of the text through a safe transmission path. However, as mentioned, Orrin teaches the header containing the minimum information needed to decrypt the ciphertext (col 8, lines 3-8). This minimum information must include region information on a starting address of the second region of the text or decryption would not be possible if the decryptor does not know where the second region starts. Further, applicant discloses that it was well known at the time the applicant's invention was made to send information through a safe transmission path (see Fig 1-2).



Art Unit: 2135

It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Orrin's invention according to the limitations recited in claim 27 because sending the region segmentation information through a safe transmission path would increase security.

**Claim 29:**

Orrin discloses a ciphertext comprising the encrypted first and second regions (col 7, line 62-col 8, line 8). Orrin does not explicitly disclose sending a cipher text through an unsafe transmission path and obtaining the safe transmission path through authentication operations. However, applicant discloses that it was well known at the time the applicant's invention was made to send cipher text through an unsafe transmission path and obtaining the safe transmission path through authentication operations (see specification, p3, paragraph 9).

It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Orrin's invention according to the limitations recited in claim 29 because the text is already encrypted, so sending it through an unsafe path would be faster than sending it through a safe path. Further, using authentication to obtain the safe transmission path would ensure that the path is actually safe, i.e. that an imposter is not asking for the secure path.

**Claim 32:**

Orrin does not explicitly disclose the region segmentation information, the information related to the second key, and the first encryption key are received through a safe transmission path. However, Orrin discloses that the header contain information

Art Unit: 2135

necessary to decrypt the cipher text (col 8, lines 3-8). This reads on the region segmentation information and information related to the second key. Further, applicant discloses that it was well known in the art at the time applicant's invention was made to send information and keys through a safe transmission path (Fig 1-2).

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Orrin's invention according to the limitations recited in claim 32 because it would increase the security of Orrin's invention.

**Claim 33:**

Orrin does not explicitly disclose receiving the encrypted text through an unsafe transmission path. However, applicant discloses that it was common in the art at the time applicant's invention was made to have received the encrypted text through an unsafe transmission path (specs, p3, paragraph 9). It would have been obvious to one of ordinary skill to have modified Orrin's invention according to the limitations recited in claim 33 because it would unsafe transmission paths are typically faster than safe paths and it would allow the message to be received faster.

**Claim 35:**

Claim 35 recites a limitation substantially similar to what is recited in claim 15 and is rejected for the same reasons.

**Claim 41:**

Orrin discloses a first encryption key (col 7, lines 62-67). Orrin further discloses decryption is the reverse of the encryption operation (col 9, lines 34-36). Note the encryption operation discussed in claim 1 as being disclosed by Orrin.

Orrin does not explicitly disclose the limitations of:

1. An authenticator to obtain a safe transmission path through which a first encryption key, region segmentation information, and information related to a second encryption key are received.
2. A decryptor to decrypt a portion of the encrypted text using the first encryption key and the region segmentation information, to extract the second encryption key from the decrypted portion using the information related to the second encryption key, and to decrypt another portion of the encrypted text using the second encryption key.

However, an authenticator to obtain a safe transmission path and an decryptor to decrypt an encrypted text was disclosed as applicant as well known in the art at the time applicant's invention was made as parts of a conventional encryption apparatus (specs, p2, paragraph 4). In light of the above teachings by Orrin and applicant's admittance of prior art, it would have been obvious to one of ordinary skill in the art at the time applicant's invention was made to have modified Orrin's invention according to the limitations recited in claim 41. One of ordinary skill would have been motivated to do so

Art Unit: 2135

as the limitations not explicitly disclosed by Orrin are the typical components necessary in an encryption/decryption apparatus.

**Claim 42:**

The limitations recited in claim 42 are a combination of what are recited in claims 7 and 33 and are rejected for the same reasons.

**Claim 43:**

Orrin does not explicitly disclose the receiver comprises an information appliance. However the examiner asserts that computers being receivers in a cryptographic system was well known at the time the applicant's invention was made. Computers are information appliances. It would have been obvious to one of ordinary skill to have modified Orrin's invention such that the receiver is an information appliance/computer because it would allow for automated cryptographic processing.

**Claim 44:**

Orrin does not explicitly disclose the receiver comprises a computer. However the examiner asserts that computers being receivers in a cryptographic system was well known at the time the applicant's invention was made. It would have been obvious to one of ordinary skill to have modified Orrin's invention such that the receiver is a computer because it would allow for automated cryptographic processing.

**Claim 45:**

Orrin does not explicitly disclose wherein the receiver comprises a server. However, servers were well known in the art at the time applicant's invention was made. It would have been obvious to one of ordinary skill to have modified Orrin's invention

such that the receiver is a server as Orrin's teachings would allow for secure communication between a client and server.

Claims 6, 9, 14, 23, 26, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Orrin (US 6,011,849) in view of McGough (US 6,445,797).

**Claim 6:**

Orrin does not explicitly disclose wherein a size of the first encryption key is fixed and a size of the second encryption key is varied by a transmission unit within the first region. However, the examiner asserts that keys of fixed and varied lengths were well known in the art at the time the applicant's invention was made.

Further, McGough discloses a cryptographic system employing the use of two keys. The size of the first encryption key is fixed (col 4, lines 59-61) and the size of the second encryption key is variable (col 4, lines 39-46). In light of McGough's teachings, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Orrin's invention according to the limitations recited in claim 6. Note that the transmission unit within the first region reads on information needed to decrypt the message, which Orrin discloses is located in the header, i.e. first region, of his encrypted message (col 7, line 65-col 8, line 8). One of ordinary skill would have been motivated to do so as McGough discloses that his teachings would guarantee a mathematical and process impossibility of ever

Art Unit: 2135

discovering or deriving the original key from the message key, making the only attack point of the system of no value (col 4, lines 46-50).

**Claim 9:**

Orrin does not explicitly recite wherein the position and size information of the second encryption key are varied. However, this limitation is obvious to the combination invention of Orrin and McGough. Note that in the combination invention, the second key size is varied. Further, Orrin discloses that the header contains the minimum information needed to decrypt the cipher text (col 8, lines 3-8). To decrypt the cipher text, one would need to know the position and size of the variable length second key. This information being variable values reads on the limitation recited in claim 9.

**Claim 14:**

Claim 14 recites a limitation substantially similar to the one recited in claim 6 and is rejected for the same reasons.

**Claim 23:**

Claim 23 recites a limitation substantially similar to what is recited in claim 6 and is rejected for the same reasons.

**Claim 26:**

Claim 26 recites a limitation substantially similar to what is recited in claim 9 and is rejected for the same reasons.

**Claim 34:**

Claim 34 recites a limitation substantially similar to what is recited in claim 6 and is rejected for the same reasons.

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

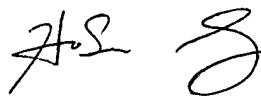
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ponnoreay Pich  
Examiner  
Art Unit 2135

  
Primary Examiner  
Art Unit 2135

PP